IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,

v. 21-CR-7-V

JOHN STUART,

Defendant.

GOVERNMENT'S RESPONSE TO
DEFENDANT'S MOTION TO COMPEL DISCOVERY

THE UNITED STATES OF AMERICA, by and through its attorney, Trini E. Ross, United States Attorney for the Western District of New York, David J. Rudroff, Assistant United States Attorney, of counsel, hereby responds to the defendant's supplemental motion to suppress and for a *Franks* hearing. Dkt. 89.

STATEMENT OF FACTS AND PROCEDURAL HISTORY

A. The Investigation:

This FBI investigation began as a lead derived from a larger investigation. Specifically, the FBI received information from a foreign law enforcement organization ("FLA") who dismantled several child pornography websites on the Tor network, also referred to as the "dark web." During the June 2019 operation, international law enforcement captured the IP addresses of visitors on the dismantled websites. These IP addresses were disseminated to the appropriate countries and, in the United States, to the districts with venue to prosecute.

One such IP address was registered to 1010 Cleveland Drive, Cheektowaga, New York. The information provided included the name of the website (the "Target Website"), a description of it as a "child pornography bulletin board and website dedicated to the advertisement and distribution of child pornography and the discussion of matters pertinent to the sexual abuse of children." The website was in operation from approximately October 2016 through June 2019, was located outside of the United States, was seized by the foreign law enforcement authority, and the IP address registered to the defendant's residence accessed the site on a particular date and time. The content of the Target Website was verified by the FBI while it was still in operation, which confirmed the site's self-described purpose to "share cp of babies and toddlers," as well as how it functioned to allow users to make and view postings that contained text, images, video images, and web links directing users to specific content at other websites. Investigators accessed the site and downloaded digital child pornography content accessible via the website in an undercover capacity.

The June 2019 lead regarding the IP address at the defendant's residence was transmitted to FBI Buffalo in July 2020. Shortly thereafter, the government obtained authorization to use a pen register and trap and trace device ("PRTT") on the target broadband account registered at 1010 Cleveland Drive, Cheektowaga, New York. The PRTT monitored the IP activity on the defendant's residence between August and October 2020. The result of the PRTT confirmed an occupant of the residence was utilizing an internet-connected device to frequent the Tor network.

The FBI obtained a federal search warrant on October 8, 2020, for the residence at 1010 Cleveland. *See* 20-MJ-5207 (under seal). The search warrant authorized the seizure and

subsequent search of the contents of electronic devices. FBI executed the search warrant on October 19, 2020. During the search, law enforcement seized electronic devices, a large amount of marijuana, marijuana plants and associated hydroponic growing supplies, psilocybin mushrooms, and firearms. An investigator interviewed the defendant during the search, during which the defendant made several inculpatory statements.

B. The Charges:

On October 20, 2020, the defendant was charged with several narcotics, firearm, and child pornography offenses. Dkt. 1. A federal Grand Jury subsequently indicted the defendant on: one count of receipt of child pornography (18 U.S.C. §§ 2252A(a)(2)(A) and 2252A(b)(1); four counts of possession of child pornography (18 U.S.C. §§ 2252A(a)(5)(B) and 2252A(b)(2); one count of possession of a firearm and ammunition by a controlled substance user (18 U.S.C. §§ 922(g)(3) and 924(a)(2); one count of manufacturing marijuana (21 U.S.C. §§ 841(a)(1) and 841(b)(1)(D); and one count of maintaining a drug-involved premises (21 U.S.C. § 856(a)(1). Dkt. 8.

C. Prior Motion Practice:

The defense moved to, among other things, suppress evidence found during the search of his home. Dkt. 27. The defendant argued that the search warrant was not supported by probable cause because, as relevant here, the government had not established the reliability of the FLA that generated the lead. Dkt. 27-2 at 1-5. In support of his motion, the defendant raised many of the same questions he raised in his most recent motion to compel discovery, *e.g.* the identity of the FLA, the investigative techniques used, what information was gathered by the FLA, etc., contending that the lack of answers rendered the FLA unreliable. *See id.* at

4. Alternatively, the defendant requested discovery on those very issues, claiming the information was material to preparing a defense—particularly his need to "properly litigate the pertinent Fourth Amendment issues before the Court, including addressing matters of reliability and veracity." *Id.* at 5.

This Court issued a Report and Recommendation in which it recommended that the District Court deny the defendant's motions. *Id.* As relevant here, the Court noted that a tip from an FLA is unlike an ordinary confidential informant. Instead, the FLA's status as a law enforcement agency, taken together—as it was here—with corroborating information obtained by the agents, is sufficient to establish that the FLA's information is reliable. *Id.* at 5-7. Judge Vilardo agreed and denied the defendant's motions. Dkt. 44.

The defendant then moved to compel further discovery. Dkt. 55. He specifically requested disclosure of:

1. The identity of the FLA that issued the tip or information;

2. The identity of the FLA that seized the computer server hosting the target website;

3. The author of the FLA notification;

4. The identity of the U.S. law enforcement agency that received the notification;

5. The complete content of the notification, including information or tactics and techniques used by the FLA to determine the identity of the IP addresses accessing the website, and any documentation/memorandum/agreement regarding the investigative technique used;

6. The number of tips provided to the United States by the FLA as part of the investigation;

7. The number of IP addresses identified as part of the investigation;

8. Any record of action taken in response by the United States to the FLA notification;

9. Any documentation/memorandum/agreement regarding collaboration between the United States and *all* FLAs involved in the investigation;

10. All cover sheets, correspondence, or other documentation documenting the totality of the tip/information provided by the FLA.

Id. The government maintained that the information requested is not discoverable, but nonetheless provided additional documents pursuant to a protective order in an act of good faith. The defendant then submitted further briefing in which he contended that the government's good faith production did not satisfy his motion to compel. Dkt. 80. In that memorandum, the defendant further requested—for the first time—that the Court order a *Franks* hearing and re-open the defendant's previously-filed motion to suppress. Dkt. 80 at 5-7. The Court directed further briefing. Dkt. 81.

D. The defendant's renewed motion to suppress:

The defendant again moves to suppress evidence seized from his home, or for a *Franks* hearing. Dkt. 89. The defendant asserts that a *Franks* hearing is necessary for three reasons: (1) the warrant application did not specify that the homepage of the Target Website did not, itself, contain child pornography; (2) the warrant application did not disclose that two FLAs were involved in the investigation, rather than one; and (3) the defendant contends that U.S. law enforcement was engaged in a "joint venture" with the FLAs. Dkt. 89 at 6-14.

The defense further urges that, considering the information now proffered in this motion, the affidavit in support of the search warrant application is unreliable. The defendant

therefore moves to re-open and grant his prior motion to suppress the evidence seized from his house. Dkt. 89. 15-19.

For the reasons discussed below, none of the defendant's claims entitles him to a *Franks* hearing. Each asserted omission or misrepresentation is either factual incorrect, or legally irrelevant. Most importantly, nothing proffered by the defense vitiates the probable cause on which the warrant was issued. The Court should deny the defendant's motions in their entirety.

ARGUMENT

A. THE DEFENDANT'S MOTIONS ARE UNTIMELY.

As an initial matter, the Court should deny the defendant's motions because they are untimely. Federal Rule of Criminal Procedure 12(c)(1) permits a court to set a deadline by which the parties are required to file pretrial motions. If the court sets such a deadline, Rule 12(b)(3)(C) requires that any suppression motions be filed by that deadline if the basis for the motion is then reasonably available. Fed. R. Crim. P. 12(b)(3)(C). If a party fails to file a suppression motion by the pretrial motions deadline set by the court, the motion is untimely unless the party "shows good cause" for the late filing. Fed. R. Crim. P. 12(c)(3). Without establishing good cause for the untimely filing, the party has waived the issue. *United States v. Mustafa*, 753 F. App'x 22, 44 (2d Cir. 2018); *see United States v. Moore*, 541 F. App'x 37, 39 (2d Cir. 2013) (affirming district court's decision to not entertain a suppression motion filed eight months after the court's pretrial filing deadline); *United States v. Howard*, 998 F.2d 42, 51–52 (2d Cir. 1993) (affirming denial of leave to file late suppression motion when filing was made thirty-nine days late).

"To satisfy the 'good cause' standard of Rule 12(c)(3) defendant must establish that the basis for the motion was not (and could not have been) known before the expiration of the motion deadline." *United States v. Sanders*, No. 19-CR-125-RJA-JJM, 2020 WL 8513483, at *3 (W.D.N.Y. Oct. 9, 2020) (citing *United States v. Robinson*, 357 F. Supp. 3d 221, 224 (E.D.N.Y. 2019) ("[T]he analysis of whether a suppression claim has been preserved focuses on whether the particular ground for suppression pressed later could have been, but was not, advanced prior to the expiration of the Court-mandated guidelines[.]")). "A strategic decision by counsel not to pursue a claim, inadvertence of one's attorney, and an attorney's failure to timely consult with his client are all insufficient to establish 'cause.'" *United States v. Yousef*, 327 F.3d 56, 125 (2d Cir. 2003). Additionally, "[C]ourts have held that counsel's failure to conduct proper pretrial investigation does not establish good cause for a defendant's failure to raise an argument covered by Rule 12(b)(3) in a timely fashion." *United States v. Gerace*, No. 19-cr-227 JLS (MJR), 2022 WL 19003139, at *4 n.7 (W.D.N.Y. Dec. 19, 2022) (citing *United States v. Duncan*, 18-CR-289, 2019 WL 5824205, at *7 (S.D.N.Y. Nov. 7, 2019)).

Here, pursuant to Rule 12(c)(1), the Court ordered that all pretrial motions must be filed by October 4, 2021—nearly 18 months before this motion was filed. As such, the defendant must show "good cause" why this motion is not untimely. He has failed to do so. Indeed, the defense does not appear to address the timeliness of its motions anywhere in its brief. That alone should be enough to deny the motion. Nevertheless, to the extent the defendant may assert that the basis for this motion was not known until the government produced additional discovery, that is also meritless. The defendant himself certainly knew what child pornography websites he was visiting. He therefore knew that the homepage of

the Target Website did not feature explicit child pornography. He was therefore also capable of undertaking the same internet searches he undertook in preparing this motion and finding the public records that he cites here. *See* Dkt. 89 at 13 n.3-6. In fact, the press release cited by the defendant that purportedly establishes a collaborative investigation was published in January 2020, references by name the Target Website, and is easily found in a Google search. *Id.* This information was therefore available to the defense well before the pretrial motions deadline in the exercise of due diligence.

At the very least, this information should have alerted the defendant to the alleged need for the discovery he now seeks and prevented him from alerting the Court that his discovery concerns had been addressed and his pretrial motions could be resolved. *See* Dkt. 33 (Report and Recommendation) at 1, n. 2.

For all of these reasons, the defendants' most recent motions to suppress and for a *Franks* hearing are untimely and should be denied as such.

B. A *FRANKS* HEARING IS NOT WARRANTED.

The Court should next reject the defendant's motion for a *Franks* hearing because the defendant failed to proffer any omissions or misrepresentations there were designed to intentionally mislead the Magistrate or that showed a reckless disregard for the defendant's Fourth Amendment rights. Even if the defendant were able to present such evidence, the omissions identified by the defendant were not material to the Magistrate's finding of probable cause.

To that end, a defendant who alleges material omissions in a warrant application can seek a *Franks* hearing only in limited circumstances. *See Franks*, 438 U.S. at 164–72. "To be entitled to a *Franks* hearing, a defendant must make a substantial preliminary showing that: (1) the claimed inaccuracies or omissions are the result of the affiant's deliberate falsehood or reckless disregard for the truth; and (2) the alleged falsehoods or omissions were necessary to the judge's probable cause finding." *United States v. Salameh*, 152 F.3d 88, 113 (2d Cir. 1998) (citations omitted).

As to the first requirement, the defendant must show that the misrepresentations or omissions were made intentionally to mislead the Magistrate or with reckless disregard. *See United States v. Awadallah*, 349 F.3d 42, 64 (2d Cir. 2003). "[A]llegations of negligence or innocent mistake are insufficient." *Falso*, 544 F.3d at 126 (citing *Leon*, 468 U.S. at 171). Additionally, "mere intent to exclude information is insufficient." *Awadallah*, 349 F.3d at 67. To illustrate the distinction between "intent to exclude" and "intent to exclude for the purpose of misleading," the *Awadallah* court cited *United States v. Colkley*, 899 F.2d 297, 300–01 (4th Cir. 1990):

> "[E]very decision not to include certain information in the affidavit is 'intentional' insofar as it is made knowingly. If . . . this type of 'intentional' omission is all that *Franks* requires, the *Franks* intent prerequisite would be satisfied in almost every case . . . . [Rather,] *Franks* protects against omissions that are *designed to mislead*, or that are made in *reckless disregard of whether they would mislead*, the magistrate."

Awadallah, 349 F.3d at 67–68 (citing *Colkley*, 899 F.2d at 300–01) (emphasis in original).

As to the second requirement, the court must determine whether the alleged misrepresentations or omissions were material to the finding of probable cause. *See Awadallah*, 349 F.3d at 64. To assess materiality, "the ultimate inquiry is whether, after putting aside erroneous information and correcting material omissions, there remains a residue of independent and lawful information sufficient to support a finding of probable cause[.]" *United States v. Rajaratnam*, 719 F.3d 139, 146 (2d Cir. 2013) (citations omitted). "If, after setting aside the allegedly misleading statements or omissions, the affidavit, nonetheless, presents sufficient information to support a finding of probable cause, the district court need not conduct a *Franks* hearing." *Salameh*, 152 F.3d at 113.

1. The warrant application did not omit information regarding the defendant's conduct or the nature of the Target Website.

The defendant first contends that "Officer Hockwater omitted the crucial fact that the homepage of the [Target Website] did not display any child sexual abuse material." In the defendant's view, because the tip from the FLA does not state that the defendant navigated past the homepage of the Target Website, the application "misrepresented the information available to U.S. law enforcement and created a misleading impression that U.S. law enforcement had more evidence of criminal activity than it actually did." This is meritless.

To begin, the affidavit in support of the warrant application, read as a whole, does not create a misleading impression as to the government's knowledge at all. TFO Hockwater stated that the tip provided by the FLA provided that an identified IP address "was used to access online child sexual abuse and exploitation material" on the Target Website. Dkt. 89-

1 ¶ 24. This is objectively true, as the quote in the application is taken directly from the FLA tip.[1]

TFO Hockwater went on to state that the Target Website was generally not accessible through the traditional internet, but rather through the Tor Network. *Id.* ¶ 28. He specified that Tor Network websites are not indexed, and therefore generally not "searchable," in the ordinary sense. *Id.* A TOR user who wanted to access the Target Website needed to find the 16 or 56-character web address of the Target Website, which would need to either be previously known to the user, or found through a directory that would "often identify . . . whether child pornography imagery may be found [on a website], and even what types of child pornography are accessible." *Id.* Thus, TFO Hockwater concluded that "because accessing the TARGET WEBSITE required numerous affirmative steps by the user—to include downloading Tor software, accessing the Tor network, finding the web address for TARGET WEBSITE, and then connecting to TARGET WEBSITE via Tor—it is extremely unlikely that any user could simply stumble upon TARGET WEBSITE without understanding its purpose and content." *Id.* ¶ 30. TFO Hockwater's overall conclusion was therefore that "there [was] probable cause to believe that . . . any user who accessed the TARGET WEBSITE has, at a minimum, knowingly accessed the TARGET WEBSITE with intent to view child pornography, or attempted to do so."

[1] This entire analysis also assumes that TFO Hockwater was actually aware that the homepage of the Target Website did not contain explicit child pornography, which is necessary to the defendant's claims. The defendant has not established that TFO Hockwater intentionally or recklessly omitted the information discussed, let alone did so with the intent to deceive the issuing Magistrate.

The warrant affidavit was not therefore misleading at all. To the contrary, TFO Hockwater laid out the exact language of the FLA tip, his knowledge (whether direct or relayed to him by other law enforcement) regarding the nature of the Target Website and how a user would access it, and his conclusion that one who accessed the Target Website did so to access child pornography. Taken together with his general knowledge that those who access child pornography generally collect and hoard it in their homes (*Id.* ¶ 41), there was ample probable cause to believe that evidence of child pornography offenses would be located at the defendant's residence.

Additionally, even if the Court find that TFO Hockwater omitted the fact that there was no child pornography on the Target Website homepage, such an omission is hardly material to the Magistrate's finding of probable cause. Indeed, probable cause does not require certainty, but only a "fair probability" that contraband or evidence of a crime will be found. *See Illinois v. Gates*, 462 U.S. 213, 238 (1983). The Court therefore did not need to know to what degree the defendant accessed the Target Website, given the nature of the Target Website, the Tor Network, and the affirmative steps needed to access the Target Website. Even if the government did not have evidence that the defendant navigated past the Target Website's homepage, and the Court knew that, the most logical conclusion would still be that he visited the Target Website to access, view, or obtain child pornography. Moreover, viewed in conjunction with the characteristics common to those who view child pornography, there would still be probable cause to believe evidence of child pornography crimes would be located at the defendant's residence.

2. The existence of a second FLA does not vitiate probable cause.

The defendant next argues that the warrant application "omitted important information about the origin of and reliability . . . of the FLA tip." Dkt. 89 at 9-11. In the defendant's view, probable cause could not be found where the reliability of the FLA that physically seized the Target Website server had not been vouched for. This, too, is meritless.

First, the defendant has again failed to establish—or even allege—that TFO Hockwater was aware of the involvement of a second FLA at the time of the warrant application. The defendant has therefore failed to establish that the omission of this information in the affidavit was intentional and omitted to deceive the issuing Magistrate.

Secondly, however, any alleged omission is immaterial. This Court has already found—and the District Court agreed—that the FLA's tip provided probable cause to issue the search warrant at issue here. *See* Dkts. 33 and 44. The Court found that where, as here, the FLA has a long history of providing reliable and actionable information to U.S. law enforcement, and the information underlying the warrant application was partially corroborated through a PRTT, the government has established the reliability of the FLA and probable cause to issue the warrant exist. Dkt. 33 at 5-7.

The defendant does not explain why the involvement of a second FLA disturbs this analysis. Indeed, the Court previously found that the tip provided by the FLA was reliable when it had *no information at all* regarding the basis of the FLA's information. This was due, in part, to the fact that foreign law enforcement is awarded a degree of inherent reliability. *See, e.g., United States v. Tirinkian*, 502 F. Supp. 620, 626 (D.N.D. 1980), *aff'd sub nom*, 686 F.2d

653 (8th Cir. 1982) (the reliability of the Royal Canadian Mounted Police is "inherent because of its status as a law enforcement agency"). How, then, would the fact that this investigation involved another FLA—acting in its official law enforcement capacity—make that tip less reliable? It would not. In fact, Exhibit D to the defendant's motion (the accuracy or authenticity of which the government cannot confirm) seems to corroborate that the investigation (a) did not involve a search of a U.S. computer, and (b) was conducted in accordance with the laws of foreign countries. *See* Dkt. 89-4. Thus, even if the involvement of the second FLA were relevant, it would make the FLA tip more reliable, not less.

In sum, nothing proffered by the defendant with respect to the involvement of the second FLA was material to the Magistrate's probable cause finding, even assuming this omission was intentional or reckless. A *Franks* hearing is therefore unnecessary.

3. The warrant application did not misrepresent the relationship between U.S. and foreign law enforcement.

Lastly, the defendant argues that the government misrepresented the degree of cooperation between U.S. and foreign law enforcement in the search warrant application. Dkt. 89 at 11-14. Had the relationship between U.S. and foreign law enforcement been disclosed to the issuing Magistrate, he argues, the warrant would not have been issued. This is also meritless.

"[T]he Fourth Amendment and its exclusionary rule do not apply to the law enforcement activities of foreign authorities acting in their own country." *United States v. Busic*, 592 F.2d 13, 23 (2d Cir. 1978); *see United States v. Lee*, 723 F.3d 134, 140 (2d Cir. 2013).

Evidence acquired by foreign law enforcement will only be suppressed where: (1) "the conduct of foreign officials in acquiring the evidence is so extreme that it shocks the judicial conscience" and (2) "cooperation with foreign law enforcement officials may implicate constitutional restrictions." *Lee,* 723 F.3d at 140. "[U]nder the 'constitutional restrictions' exception, constitutional requirements may attach in two situations: (1) where the conduct of foreign law enforcement officials rendered them agents, or virtual agents, of United States law enforcement officials; or (2) where the cooperation between the United States and foreign law enforcement agencies is designed to evade constitutional requirements applicable to American officials." *United States v. Getto*, 729 F.3 d 221, 230 (2d Cir. 2013).

As an initial matter, the Court should reject the defendant's attempts to apply the "joint venture doctrine" in this case.[2] Although the joint venture doctrine has been applied by some Circuit Courts "with inconsistent, even confusing, results," (*Getto*, 729 F.3d at 233), the Second Circuit has consistently refused to adopt it. *See id.* ("[w]e have repeatedly declined to adopt the joint venture doctrine in the context of the Fourth Amendment . . . [w]e, therefore, decide again not to adopt the joint venture doctrine."). Instead, the Second Circuit holds that "the longstanding principles of 'virtual agency' and intentional constitutional evasion . . . [are] the applicable analytic rubric to determine whether 'cooperation with foreign law enforcement officials may implicate constitutional restrictions.'" *Id.* (*citing Lee*, 723 F.3d at 140); *see United States v. Maturo*, 982 F.2d 57, 60-61 (2d Cir. 1992).

[2] The joint venture doctrine applies the exclusionary rule to foreign law enforcement action where "United States agents' participation in the investigation is so substantial that the action is a joint venture between United States and foreign officials." *United States v. Peterson*, 812 F.2d 486, 490 (9th Cir. 1987); *see United States v. Valdivia*, 680 F.3d 33, 52 (1st Cir. 2012).

Applying the *Lee* analysis, nothing proffered by the defendant warrants suppression or a *Franks* hearing. First, with respect to whether foreign law enforcement action shocks the judicial conscience, the defendant has again offered nothing to support his baseless claim that foreign law enforcement used a NIT to de-anonymize Tor Network users. Although the government does not know the methodology used by the FLA to identify the defendant's IP address, we have been assured that it was not a NIT. This was unequivocally stated to the government by the lead FBI Special Agent assigned to this investigation and has been repeatedly proffered to the Court and the defense.

Moreover, nothing in defendant's Exhibit D (assuming that it is an accurate account of the foreign investigation) shocks the judicial conscience. Instead, that document recounts a series of international tips culminating in investigative steps taken pursuant to the investigating country's laws. All of which led to the FLA providing a tip to the FBI and the issuance of a warrant to search the defendant's residence for child pornography.

Turning to the second *Lee* prong, again, nothing proffered by the defendant even presents a question as to whether the foreign investigation implicated constitutional restrictions. At most, the defendant's proffer establishes a history of effective information sharing between U.S. and foreign law enforcement. It does not, however, suggest that foreign law enforcement acted as "virtual agents" of U.S. authorities, or that the cooperative relationship was designed to evade constitutional requirements applicable to a domestic FBI investigation. Again, no foreign law enforcement undertook investigative action at U.S. direction. No U.S. law enforcement personnel participated in foreign searches or seizures. The warrant at issue was the product of efficient and effective information sharing.

The probable cause underlying the search warrant in this case would still exist even if the application had included all of the information proffered by the defendant. Any ostensible omission was not, therefore, material, and a *Franks* hearing is not necessary.

C. THE COURT SHOULD DENY THE MOTION TO SUPPRESS BECAUSE IT IS WITHOUT MERIT, AND, IN ANY EVENT, THE GOOD FAITH EXCEPTION WOULD APPLY.

As the government noted in point B.2, above, this Court already found that probable cause supported the issuance of the search warrant at issue. The affidavit submitted in support of the search warrant application established that the FLA tip was reliable, both because of the inherent credibility of foreign law enforcement and the corroborating established through a PRTT. The defendant has not proffered any new information that would disturb that analysis. However, even assuming newly discovered information does somehow vitiate probable cause, the Court should apply the good faith exception to the exclusionary rule.

Indeed, even if a warrant is subsequently adjudged to have lacked probable cause or otherwise to be deficient, "[s]uppression is to be the 'last resort, not [the court's] first impulse.'" *United States v. Guzock*, 998 F. Supp. 2d 102, 108 (W.D.N.Y. 2014) (quoting *Herring v. United States*, 555 U.S. 135, 140 (2009)). This is because, as the Supreme Court has noted, the "heavy toll" that the suppression of evidence takes on the administration of justice: "its bottom-line effect, in many cases, is to suppress the truth and set the criminal loose in the community without punishment." *Davis v. United States*, 564 U.S. 229, 237 (2011). Thus, "[t]o trigger the exclusionary rule, police conduct must be sufficiently deliberate that exclusion

can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system." *Herring*, 555 U.S. at 144.

As such, when evidence is obtained by law enforcement who executed a search "in objectively reasonable reliance" on a subsequently invalidated warrant, the "good faith exception" applies, and the evidence will not be suppressed. *See United States v. Falso*, 544 F.3d 110, 125 (2d Cir. 2008). This proposition is derived from *United States v. Leon*, 468 U.S. 897 (1984), in which the Court held that evidence obtained pursuant to a warrant that was later found to be defective was still admissible because law enforcement had reasonably relied on the magistrate's determination of probable cause. *Id.* at 925–26. The burden rests with the government to show that the good faith exception applies. *See United States v. Clark*, 638 F.3d 89, 100 (2d Cir. 2011). "Most searches conducted pursuant to a warrant would likely fall within [the good faith exception's] protection." *Id.* Relevant to the defendant's baseless claims, here, the good faith exception does not apply if the affiant knowingly misled the magistrate. *See id.*

Here, there is no reason to believe that TFO Hockwater knowingly or intentionally misled the Magistrate. As discussed above, nothing in the search warrant application was misrepresented to the Magistrate, and, even if the omitted information is deemed material, there is no reason to believe that TFO Hockwater knew the omissions would be material to a finding of probable cause, given the discussion above. This is also supported by the caveat in TFO Hockwater's affidavit in which he states "[s]ince this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known

to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause . . .” Dkt. 89-1 ¶ 3.

There is no record evidence to suggest that any omission was an intentional attempt to mislead the issuing magistrate. If the Court finds that the information proffered by the defendant somehow vitiates the probable cause upon which the warrant was issued, the Court should apply the good faith exception to the exclusionary rule and deny the defendant’s motion to suppress.

CONCLUSION

For all of the foregoing reasons, the government respectfully requests that the Court deny the defendant’s motion to suppress and for a *Franks* hearing.

DATED: Buffalo, New York, April 28, 2023

TRINI E. ROSS
United States Attorney

BY: ***/s/DAVID J. RUDROFF***
Assistant United States Attorney
United States Attorney’s Office
Western District of New York
138 Delaware Avenue
Buffalo, NY 14202
716/843-5806
David.Rudroff@usdoj.gov